STATE OF WISCONSIN
DEPARTMENT OF WORKFORCE DEVELOPMENT (DWD)
DWD POLICY MANUAL APM 510 11/01/98

COMPUTER SECURITY

DWD has adopted the following organizational and individual responsibilities and minimum requirements for the proper use, security and protection of DWD's computer and information assets which include the equipment, programs, software, data, personnel, facilities, documentation, and libraries.

Access is controlled for any information whose unauthorized use, disclosure, alteration or destruction could be detrimental to DWD's mission and/or is in violation of federal or state confidentiality and open records laws. Other sensitive information whose disclosure could violate a person's right to privacy also must be protected.

The following applies to all DWD computer assets. Additional requirements for micro and minicomputers are contained in APM 509. Divisions also may set their own computer security standards. Questions on security should be directed to the Automation Security Office in the Systems & Data Processing (SDP) Bureau.

Procedures and Responsibilities:

All owners and users of the information systems share the responsibility to:

- ensure that information is accurate, complete and up-to-date
- protect related communication and other peripheral equipment from physical abuse or any unauthorized use
- ensure that application and operating system programs perform according to management instructions
- ensure that new and modified applications are approved for security compliance before becoming operational
- limit access on a need to know (job function) basis
- limit use of computers or equipment off premises or outside DWD control to purposes approved under a signed equipment agreement
- prohibit reproduction or unauthorized use of proprietary software licensed to DWD.

Computer programs developed by DWD employes or contract personnel for DWD, or purchased for DWD use are state property. Programs written as part of employe job duties are DWD property and may not be distributed outside DWD unless authorized by the Secretary. This does not apply to programs written by employes on personal home computers or to authorized sharing of programs with other government units.

The following explains the organizational and operational responsibilities for computer security:

Division Management authorizes use of systems and information, ensures usage consistent with DWD and division purposes, identifies sensitive information and critical applications, monitors compliance with security policies to reduce the risk of unauthorized use, alteration or destruction of sensitive information and implements appropriate security measures to protect personnel, equipment, facilities, data, programs, libraries and documentation from losses.

Division Security Officers are appointed by the division administrator and coordinate and document the overall security of division computer facilities, systems and data, review user requests for access to systems and files, and monitor and enforce compliance with security standards.

SDP provides software and hardware necessary to ensure security, and provides guidance and assistance on backup/recovery systems.

The System Administrator is responsible for minicomputer operations, production of operational management reports, scheduling/completing data backup, monitoring security and notifying division and DWD security officers of continued security violations.

The Automation Security Office provides technical support and consultation to data owners and custodians, reviews data security and security policies as affected by technical, environmental or statutory changes, recommends and updates security standards and policies, administers access control software, and monitors compliance with policies, standards and procedures.

Employes/Users are responsible for proper use and protection of information, compliance with usage controls, reporting errors, omissions, abuses or violations of security to supervisors, system administrator or DWD security officers. Employes also may suggest improvements in security processes.

Security regulations also cover physical and computer access, information and personnel.

Physical Access:

DWD computer installations and supporting facilities must restrict physical access where continued operation is considered essential or where sensitive or confidential information is stored online.

Only authorized personnel may be admitted to an installation operations area, such as a computer room.

Access to program documentation and data storage is restricted to those with established and authorized needs.

Personnel:

Pre-employment screening is required for certain positions in SDP and the program divisions. SDP has established procedures for assessing potential security risks.

When receiving access, all users must be informed of security policies and their responsibilities to protect data, and acknowledge their understanding in writing.

Personnel terminated or suspended after disciplinary actions will be immediately excluded from access to systems. Extended absences or seasonal layoff may result in temporary denial of access.

Logical Computer Access:

Passwords are used to prevent unauthorized access to information systems.

Personally assigned passwords must be changed periodically, and those assigned for other systems should not be used for CICS and/or TSO mainframe access. Frequent changing of passwords is particularly important for users with access to confidential or sensitive data.

Passwords should be difficult to guess, balanced with the ability to remember them and ease of input. Words like HELLO, START, SYSTEM, the user's name and other words easily associated with the user or the job are prohibited. Passwords must be memorized and not written down.

Passwords are state property and users must prevent unauthorized use. If a password may have been compromised, it must be immediately changed, and the division security officer must be notified.

To prevent unauthorized use of a computer, employes should log off completely before leaving the work area. Computers and workstations should never be in an operational mode unless the user is present.

Access is suspended or modified on user termination or transfer to a position where the same access is not required.

Users may not permit unauthorized computer use by giving a password to or signing on for another person or by leaving a signed on terminal unattended.

Release of Information:

Release of data to outside agencies must be approved in accordance with APM 503 - Records Management. Divisions also may adopt more restrictive policies on data release.

Before returning rented or leased magnetic storage media to vendors, users should consider erasing or overwriting any unencrypted confidential data.

DP waste material such as printouts, tapes, diskettes, microfilm or microfiche which contain confidential records will be destroyed.

Data critical to ongoing operations and supporting continued operations in the event of a disaster (including source and object libraries, system documentation, etc.) will be regularly copied and stored off-site.

Violations:

Violations of computer security include:

- failure to follow procedures for protection, access or distribution of sensitive information
- unauthorized attempts to access or circumvent protection systems for sensitive information
- unauthorized possession of sensitive information
- manipulating and/or using data or computer time for personal gain or mismanaging computer resources (personal letters, mailing labels, bank statement reconciliations, etc.)
- using data or equipment on behalf of an organization without prior approval.

Users may be held accountable for any use or misuse of property which takes place under computer access using their logon number.

If an inquiry finds negligence or malicious intent, DWD disciplinary actions found in the Personnel Manual may be followed. Offenses also may result in prosecution under the state computer crimes law.

WISCONSIN STATE STATUTE 943.70 COMPUTER CRIMES

(1) DEFINITIONS. In this section:

(a) "Computer" means an electronic device that performs logical, arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer in a computer system or computer network.

(b) "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of 2 or more interconnected computers.

(c) "Computer program" means an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data.

(d) "Computer software" means a set of computer programs, procedures or associated documentation used in the operation of a computer system.

(dm) "Computer supplies" means punchcards, paper tape, magnetic tape, disk packs, diskettes and computer output, including paper and microform.

(e) "Computer system" means a set of related computer equipment, hardware or software.

(f) "Data" means a representation of information, knowledge, facts, concepts or instructions that has been prepared or is being prepared in a formalized manner and has been processed, is being processed or is intended to be processed in a computer system or computer network. Data may be in any form including computer printouts, magnetic storage media, punched cards and as stored in the memory of the computer. Data are property.

(g) "Financial instrument" includes any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or credit card, transaction authorization mechanism, marketable security and any computer representation of them.

(h) "Property" means anything of value, including but not limited to financial instruments, information, electronically produced data, computer software and computer programs.

(i) "Supporting documentation" means all documentation used in the computer system in the construction, clarification, implementation, use or modification of the software or data.

(2) OFFENSES AGAINST COMPUTER DATA AND PROGRAMS. (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b) :

1. Modifies data, computer programs or supporting documentation.

2. Destroys data, computer programs or supporting documentation.

3. Accesses data, computer programs or supporting documentation.

4. Takes possession of data, computer programs or supporting documentation.

5. Copies data, computer programs or supporting documentation.

6. Discloses restricted access codes or other restricted access information to unauthorized persons.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2. , 3. or 4. applies.

2. A Class E felony if the offense is committed to defraud or to obtain property.

3. A Class D felony if the damage is greater than $2,500 or if it causes an interruption or impairment of governmental operations or public communication, of transportation or of a supply of water, gas or other public service.

4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(3) OFFENSES AGAINST COMPUTERS, COMPUTER EQUIPMENT OR SUPPLIES. (a) Whoever wilfully, knowingly and without authorization does any of the following may be penalized as provided in par. (b) :

1. Modifies computer equipment or supplies that are used or intended to be used in a computer, computer system or computer network.

2. Destroys, uses, takes or damages a computer, computer system, computer network or equipment or supplies used or intended to be used in a computer, computer system or computer network.

(b) Whoever violates this subsection is guilty of:

1. A Class A misdemeanor unless subd. 2. , 3. or 4. applies.

2. A Class E felony if the offense is committed to defraud or obtain property.

3. A Class D felony if the damage to the computer, computer system, computer network, equipment or supplies is greater than $2,500.

4. A Class C felony if the offense creates a substantial and unreasonable risk of death or great bodily harm to another.

(4) COMPUTER USE RESTRICTION. In addition to the other penalties provided for violation of this section, a judge may place restrictions on the offender's use of computers. The duration of any such restrictions may not exceed the maximum period for which the offender could have been imprisoned; except if the offense is punishable by forfeiture, the duration of the restrictions may not exceed 90 days.

(5) INJUNCTIVE RELIEF. Any aggrieved party may sue for injunctive relief under ch. 813 to compel compliance with this section. In addition, owners, lessors, users or manufacturers of computers, or associations or organizations representing any of those persons, may sue for injunctive relief to prevent or stop the disclosure of information which may enable another person to gain unauthorized access to data, computer programs or supporting documentation.